Information Security Governance: An action plan for a non-profit organization based in the Nordics

Olundegun, Luqman Ayodele

2018 Laurea

Laurea University of Applied Sciences

Information Security Governance: An action plan for a non-profit organization based in the Nordics

Luqman Ayodele Olundegun
Degree Programme in Security Management
Bachelor’s Thesis
May, 2018

Laurea University of Applied Sciences **Abstract**
Degree Programme in Security Management
Bachelor's Thesis

Luqman Ayodele Olundegun

Information Security Governance: An action plan for a non-profit organization based in the Nordics

Year	2018	Pages	50

This thesis examined the gaps in the Information Security Governance process of a non-profit organization based in the Nordics and identified important actions required to close the existing gaps. The maturity level of seven (7) perspectives from the ISO 27002 relevant to the non-profit organization was assessed using the COBIT maturity model to determine the gap between the current and desired level of the organization's governance process. Five (5) Country representatives and three (3) Managers from 5 countries (Finland, Sweden, Denmark, Norway, and Iceland) were interviewed using a structured questionnaire developed based on ISO 27002 and COBIT maturity model.

The thesis adopted a combination of qualitative and quantitative research method. The data collected from the interviews were used as the primary data source and a statistical representation of the data was depicted using a Radar chart to show the current level, desired level specified by the non-profit organization and the desired level specified by the respondents during the interview.

The result of this thesis shows that the non-profit organization's supplier service delivery management, incident management and information security risk management procedures were not in place while other perspectives such as information security policy, asset classification, continuity planning and personnel security were not standardized based on COBIT maturity model. In addition, the thesis shows the gap margin between the current and the organization's desired maturity levels. The widest gap measured was in the organization's supplier service delivery management procedures while the lowest gap measured was in the organization's personnel security management procedures.

This thesis provided a prioritized list of needed actions to close the identified gaps in the organization's information security governance process to achieve its desired maturity level. The conclusion drawn from this thesis was that the non-profit organization is vulnerable to potential breaches because the non-technical governance perspectives needed to secure its information security systems were not based on any standard practice and undefined.

Finally, this thesis recommended further research of the organization's information security governance process capability supported by field study to all the units in the Nordics to determine appropriate desired maturity level for each ISO 27002 perspectives related to the organization.

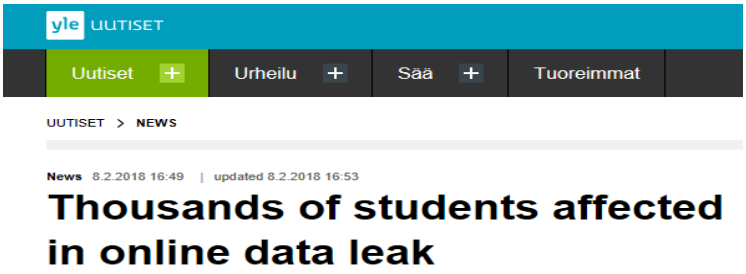
Keywords: information security governance, strategic alignment, maturity, information security organizational structure

Table of Contents

1 Introduction

The breakthrough in the information technology has made many enterprises to be dependent on internet for various daily business operations, it is now possible for a new member of an organization to register online, make an online request for membership identification, make payment for membership fee, participate in an online meetings, seminars and conferences with just a mouse click without the need for physical presence at any of the organization's branch.

Information is an essential driving force for many enterprises because of the unarguably vast benefits it offers, unfortunately, its security is being systematically breached by threat agents for valuable exploit because of poor information security governance (henceforth ISG) which poses high risk on the confidentiality, integrity, and availability of enterprise's proprietary information, financial and other intangible assets.
It appears that enterprises are helpless given the number of successful attacks lately. For instance, enterprises such as Equifax, Adult Friend Finders, eBay, and others had been victims of data breaches by hackers with yahoo described as the biggest victim of the 21st century.



UUTISET > NEWS

News 8.2.2018 16:49 | updated 8.2.2018 16:53

Thousands of students affected in online data leak

Figure 1: Screenshot from Yle Uutiset Website

In 2018, thousands of matriculation students' information was reportedly leaked in Finland because of the security breach in the examination board's online server. Yle Uutiset quoted Helsinki Sanomat report that approximately 7,695 students' personal information including names, addresses, phone numbers, study information and social security numbers was leaked. This raises a lot of concern about the security of personal information in other organizations.

Previous information security breaches had shown that breaches are a global challenge that concerns both government and non-profit organizations.

"If these hacks are happening to the biggest, most well-recognized and well-funded businesses and nations, then what chances do the relatively smaller cyber targets have at protecting themselves?" Donaldson et al. 2015

Gelles (2015) quoted John Chambers who states that there is no completely secure data centre or network that has not experienced information security incident, meaning no enterprise is completely secure, and the number of attacks is exponentially growing. Inadequate ISG often leads to inconsistencies in systems configuration and it has been identified as a major cause of the security incidents experienced by many enterprises.

The value of information cannot be overemphasized. According to the report of a global benchmark study conducted by Ponemon Institute in 2017, the average total cost of the data breaches was $3.62 million representing a 10% drop from the average total cost in 2016. The report valued the cost of each lost data containing sensitive information at $141 in 2017 serving as a multiplier for the financial estimation of every data loss by an organization.

Many enterprises appear to be secured and protected because of the investment in technology, processes, and people used to protect enterprise's information assets and other business assets, against disclosure from unauthorised users, improper modification, and denial of access whenever the information is required, but security breaches are still hardly not recorded in a week.

While many enterprises heavily invest in the deployment of sophisticated IT infrastructures and technical solutions to protect their information assets, they failed to provide effective governance and identify gaps in their enterprise information security program which in most situations have legal, financial, and reputational consequences especially, when the confidentiality, integrity, or availability of information is compromised.

An effective ISG may be impossible without the absolute commitment of the senior management of an enterprise to complement the technical measures such as firewalls, biometric, Intrusion Detection Systems (IDS), server isolation and backups often deployed to mitigate the threats to information – by providing leadership for the protection of enterprise's information assets, assigning responsibilities, providing accountability and strategic direction to mitigate information security risk to an acceptable level.

Governance like any other social science term has no universal definition. However, this thesis defines governance as the set of responsibilities and practices performed by the senior management specifically board and executive management with the objective of realizing benefits, ensuring risk optimization, and verifying that organization resources are responsibly used by optimizing cost. This includes practices and activities aimed at providing strategic direction for information security (Whitman & Mattord 2016).
Senior management of an enterprise needs to identify a combination of control measures and best practices based on profound ISG framework and standards that allows governance maturity level assessment.

There are different models for measuring the maturity of enterprise ISG, but which model will provide an integrated approach for a non-profit organization is still a matter of concern. Information security has both technical and non-technical governance perspectives, however, evaluation of the technical perspectives is outside the scope of this thesis rather this thesis will focus on the non-technical governance perspectives specified by the ISO/IEC 27000 family of standards and COBIT framework. The main purpose of this thesis is to determine the gaps in a non-profit organization ISG process and identify the important issues to be considered in developing a roadmap for closing the prevailing gaps.

Therefore, this thesis is a suitable guide for the board of directors, senior management, country manager/representatives and stakeholders providing strategic leadership for the information security of organization X which is the anonymous name of the non-profit organization used as a case study for this thesis.

lastly, it is important to clarify some of the ambiguity on what is considered an enterprise. Harmer (2013) clarifies that an enterprise is a term that describes a range of different organizations including corporations established for commercial purposes which may or may not be listed on the stock exchange, public sector organization such as a local or national government establishment, or a non-governmental organization established for a non-profit purpose. Therefore, these two terms; enterprise and organization can be interchangeably used as a generic term that covers government, private, and non-government organizations.

1.1 Research Question

The research questions for this study are coined in accordance to the research interest of Organization X. The aim is to point the research towards providing answers to the following questions which are considered vital to the creation of organization X's information security governance roadmap:

1. What is the gap in the Organization X's information security governance?
2. What is the current level of information security governance of Organization X?
3. What is the desired level of the Information security governance of Organization X?

2 Theoretical Framework

In this chapter, previous literature will be reviewed to provide theoretical background for this study.

2.1 Information Security Governance(ISG)

ISG is an established component of corporate governance because ISG is a subset of enterprises' corporate governance (Von Solms R. & Von Solms S. H. 2006). More specifically, corporate governance is defined as the objectives, policies, processes, and strategies for controlling and directing an enterprise (Kearney & Kurger 2013), this includes enterprise ISG which is often viewed as a set of technical issues than corporate governance responsibilities (Swindle & Conner 2004).

Brotby (2008) conceptually describes ISG as a process governed by Senior Management, Executive Management and Chief Information Security Officer (CISO) to facilitate the strategic alignment of organization's business objectives and information security objectives. Brotby (2008) further identifies the business strategy, information security strategy, security policies, and standards as drivers of organization's strategic alignment.

Gelbstein (2012) summarizes the purpose of ISG under three key important functions which include; evaluating, directing and monitoring organization's information security to ensure business objectives requirements are met, identify information risk owners, achieve assurance integration and reduce non-compliance and litigation risks with sustainable confidentiality, integrity, and availability.

ISG is not perceived as an important issue in many not-for-profit organizations. This is evident in the outcome of a study conducted in 2005 by Aberdeen Group in the not-for profit sector which revealed that ISG is not included in the top 10 areas of concern for board members and executives. The audit tried to rank the perceived importance of ISG in the not-for-profit sector.

Some factors that may contribute to the low perceived importance of governance includes; ineffective security policies,lack of executive interest, poorly defined risk management, rapid changes in technological innovations, poor estimation of the value of information, boundaries of information security, poorly defined roles and responsibilities, and Bring Your Own Technologies such as laptops, iPods, flash drives etc.

Setting boundaries on information security involve the management's direction on defining privileges for accessing information based on roles and responsibility which is often considered as IT department responsibility or service provider's responsibility depending on the organization. The need for regular cost reductions and the resources to mitigate risk in a business environment in which threat landscape is consistently changing often demands senior management intervention in ensuring that risk acceptance falls within the organization's risk appetite.

Without a policy, standards, and blueprints organizations may find it difficult to meet the information security need of various stakeholders (Whitman & Matthod, 2016). Similarly, failure to develop an information security strategy can negatively impact organization's ability to achieve the objective of strategy which is to achieve the desired state of security.

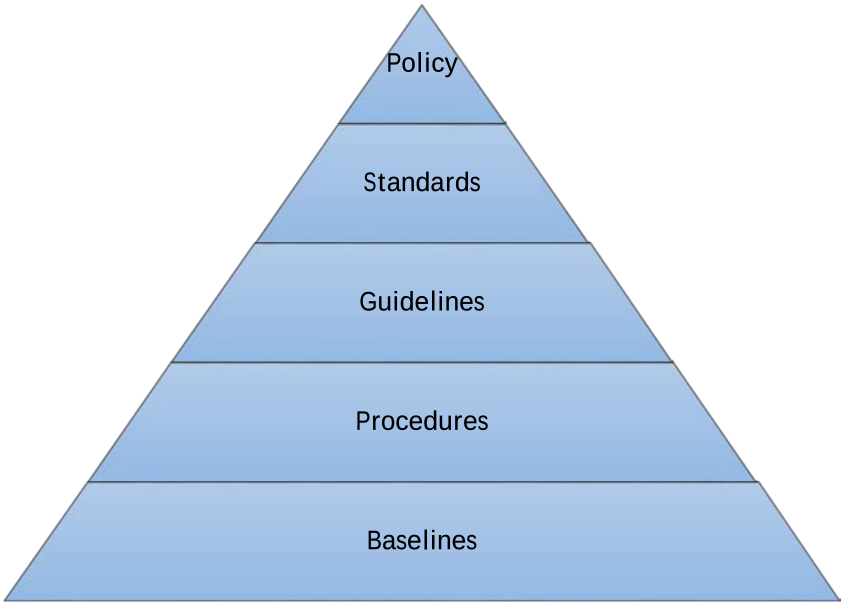


Figure 2: Pyramid of Information Security Strategy Documents

According to Osborne (2006), an organization's security policy is a list that dictates operational standards and procedures by clearly specifying the do's and don't. The policy serves as a tactical means of specifying business rules and guidelines that ensure compliance with an organization's strategic direction.

An organization's information security policy may address different aspect such as computer ethics policy, password protection policy, clean desk policy,technology disposal policy, physical security policy, electronic mail policy, removable media policy, remote access policy, internet usage policy, mobile device policy, software policy, network management policy and acceptable use policy.

ISG largely depends on sound policies backed with a suitable degree of authority and a means of auditing compliance and violations. It contains a high-level statement of principles governing enterprise information security. An enterprise security culture is often characterized by the information security policy statements. An enterprise with strong command and control security culture usually use strong imperative statement in their information security policies. For example, an enterprise information security policy may require all users to separate personal files from work-related ones using strong imperative, unambiguous and concise statement to establish intent:

All users <u>must</u> separate personal files from work-related files and stored in a separate directory marked personal (source: Users rules of Laurea IT services).

The underlined word in the example of an imperative policy statement above is only used in an enterprise with strong command and security culture. However, there are other subtle and persuasive phrases that can be used depending on the enterprise security culture (BERR 2012).
According to (Whitman & Matthod, 2016) establishment of an enterprise's information security policies, standards and practices are the ideal starting point for the creation of information security program, such creation must consider the enterprise's security architecture and select a detailed information security blueprints. Delligent Corporation (2016) suggests constant assessment and measuring of ISG to identify policies that are working and vice versa. Also, measuring and assessing organizations' Information security policies can promote identification of policy violators and compliants.

But, how is it possible to measure an organization's security policies that have not existed or been documented? Suppose it does exist and it has been documented yet it would be important to question the level of stakeholders' awareness of such policies within the organization and their ability to access it. More importantly, to identify how consistent is the policy across the organization. Most importantly, how the policies have been reviewed by the senior management and board members to address the changes in the threat landscape of the organization.

Usually, the standard gives detailed technical description or specification needed when performing a specific function (Osborne 2006 pg. 24). Standards are designed to provide policies with support and strategic direction by specifying mandatory activities, actions, rules, or regulations (Peltier 2002). Enterprise information security policies are usually based on standards, frameworks and best practices developed by International organizations such as ISO/IEC 27000 family of standards, BSI IT security baseline, COBIT, ANSI, FIPS, GASSP, ISF, ITIL etc. to help an organization achieve internal governance and reduce information security risk. Standard specifies behavior, processes, configurations, technologies needed for enterprise information security.
Also, the adoption of standards, frameworks and best practices can positively influence information security regulatory compliance (Turner & McKnight 2008).

2.2 Information Security Organizational Structure

The structure of an organization is an important success factor in its ISG, it focuses on organizing and accounting of organization's business units and departments. To a high extent, ISG is dependent on the leadership and organizational structures that safeguard information (NIST 2006). In 2018 global state of security survey, research findings reveal that only 44% of respondents confirm the active participation of boards in the organizations' overall security strategy.

Failure to coordinate and localize authority by the board of directors and/or senior management may pose challenges for organization-wide compliance on policy approval, control monitoring, performance metric reviewing and risk reduction. This may influence lower-level personnel non-abiding tendencies. To avoid non-abiding tendencies, organizations must establish top-down information security strategy (PwC GSISS 2018).

Board of directors and senior management of organizations need to periodically request and review the result of Business Impact Analysis (BIA) and other risk-related assessments to identify key organizational assets and determine criticality and dependencies in the daily business operation.
According to NIST handbook, 2006, ISG structure can be divided into two basic models; the centralized and decentralized models.

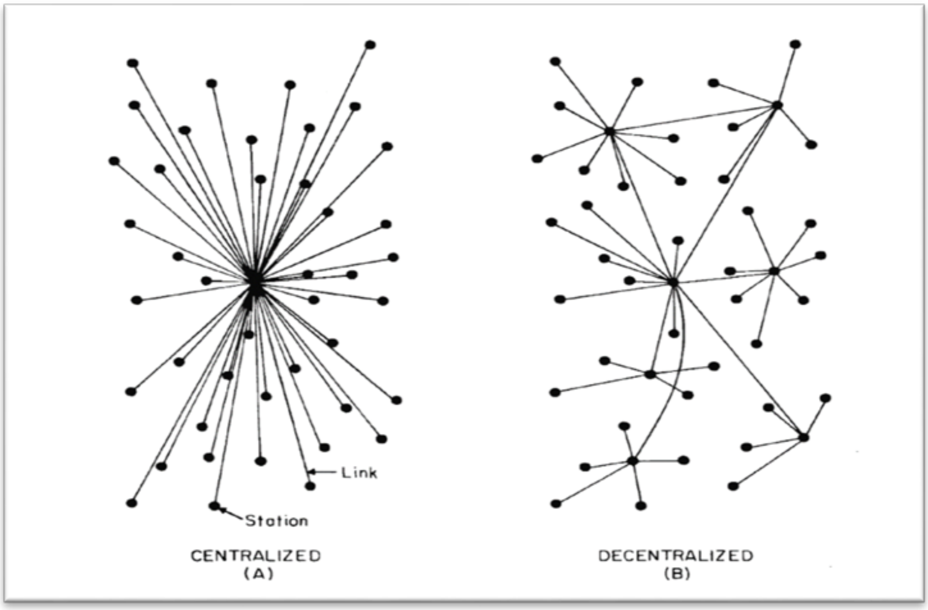


Figure 3: Baran's Centralized and Decentralized model of organizational structure Source Borowski Craig

The centralized model is characterized by the central corporate governance of policies, procedures, process, and controls that define ISG among disparate business units. Cost savings, process efficiencies, standardization and improved value delivery are some of the benefits derivable from a centralized model.

Conversely, individual business units' governance of information security programs characterizes the decentralized model. The advantage of this model is the possibility for each business units to autonomously produce policies that are tailored to their specific business model and operating environment.

Organizations with extreme diversity in terms of business operations across different geographical locations can adopt the hybrid model which is a combination of the centralized and decentralized models. Especially, where organization's policies, procedures, processes, and standards are not in conformity with the local legislation and regulatory requirements of some business units, the full compliance of the centralized model maybe partially suspended to the extent of its applicability in that business unit and a decentralized model may be activated in this situation.

2.3 Expected Outcomes

ISACA (2010) identifies six (6) major outcomes that an effective ISG should achieve, these include; strategic alignment, risk management, performance measurement, value delivery, resource management and assurance process integration.

2.3.1 Strategic Alignment

Strategic alignment between business and IT is important to improve organization's business performance (Sabherwal & Chan 2001). It involves careful consideration of how to achieve the strategic fit and functional integration of business strategy, information technology strategy, organizational infrastructure and processes, and information security infrastructure. Henderson and Venkertraman (1999) Strategic Alignment Model (SAM) provides a theoretical understanding of the Business and IT Alignment.

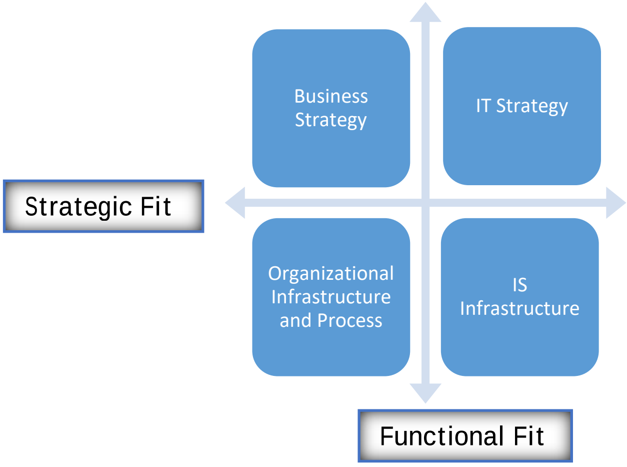


Figure 4: Henderson and Venkertraman (1999) Strategic Alignment Model (SAM)

As it can be seen in Figure 4 above, the model consists of four quadrants which are linked together by the strategic fit and functional integration linkage. The vertical linkage is the functional integration and the horizontal linkage is the strategic fit. The first and second quadrants of the SAM model shows Business Strategy and IT Strategy as an external domain which should be articulately linked with the internal domain – the combination of Organizational infrastructure and Processes, and Information System Infrastructure – to achieve strategic alignment (Henderson and Venkertraman 1999).

Business strategy is mainly concerned with the mission, vision, and objectives of an organization. IS strategy deals with the use of applications or software's and other information technology means to support an organization business objective (Chew & Gottschalk 2009). The attainment of strategic alignment can be jeopardized when IS/IT Strategy is not concurrently planned (Cassidy 2006). Therefore, an organization's management should integrate the information security practices into the organization's business processes through the expansion of corporate governance policies and controls to cover the objectives of the information security process (Whitman & Mattord 2016).

According to Hann & Weber (1996), IS/IT Strategic planning is a set of activities aimed towards achieving the following objectives:

1. Identifying organizational problems and recognizing opportunities where IS/IT might be effectively applied.
2. Finding the appropriate resources needed to enable successful usage of IS/IT to provide a solution to the identified opportunities and problems.
3. Developing strategies and procedures that will allow IS/IT to be successfully applied to the identified opportunities and problems.
4. Establishing monitoring and bonding of IT managers to ensure their actions are harmonized with the goals of their senior management.

5. Resolving problems associated with gains and losses from unforeseen circumstances will be distributed among senior management and IT Manager
6. Determining the extent of decision right to be delegated to the IT Manager.

In addition, any information security strategy should be developed with the main objective of complementing business goal through responsible management and control of the information security risk of the organization (Pironti 2010).

2.3.2 Information Security Risk Management

Information risk management is one of the major outcomes of an effective information security governance (ISACA, 2010). In theory, a risk is the probability of a threat taking advantage of a vulnerability to cause harm to an organization's asset. More specifically, it is the probability of the interaction of threats and vulnerabilities acting against an organization.

In mathematical term according to (Jones & Ashenden 2005, 186);
Risk = Threat X Vulnerability X Impact (Asset Value)
The above mathematical term simply means that:
Risk = 0 when either threat, vulnerability, or impact = 0
Risk = Likelihood (probability) X Impact

Therefore, the likelihood of a risk is greatly dependent on the availability of threat agent (attacker), vulnerability (weakness), and impact. The notion of a zero risk does not exist as organizations are incessantly faced with various threats emanating from recruiting, outsourcing, collaborating, manufacturing, marketing, and business location (Whitman & Mattord 2016). In simple term, the vulnerability is synonymous with weakness, it allows threat agents to explore or compromise an organization's information assets. Vulnerabilities can arise from human failures, failure in physical security systems or technological flaws which threat agent can quickly explore to cause harm to the information systems or process of an organization.

Just as vulnerabilities can take many forms, so too can threats, A threat can be technological, human or force majeure when it is viewed from the threat agent perspective. Also, a threat can be deliberate or accidental depending on the threat motivation. In addition, it can be internal or external when threat source is the basis of categorization.

The growth of an organization depends on how the management can effectively manage risk and protect the organization's business interest which makes risk management a critical organization's success factor (Obicci & Adoko 2017). Unfortunately, most organizations are not only clueless about the profile of their information security risk, they also lack the ability to assess it because there are many who share the notion that it is impossible to calculate it.

However, Touhill G.J & Touhill C. J. (2014) believe that some of the same techniques used to calculate risk in other sectors can be used to assess information security risk.

Quantitative and qualitative risk assessment is the popular techniques used in other sectors. In theory, quantitative risk assessment is based on numbers and complex mathematics, and qualitative risk assessment is based on scenarios and items ranking such as high, medium, or low.

For an organization to manage its information security risk effectively; first, the value of assets need to be determined. This value is often more than the capital cost. Asset value can be calculated based on the total cost of replacing the assets and the cost of possible embarrassment the organization incurred, and the cost of business loss that might be recorded by losing the asset. Mere destruction, corruption, theft, modification, removal, disclosure, or interruption of information, perhaps web codes or system log files or other resources could damage an organization's reputation.

Information Asset Classification

According to ISO 27001, information assets can include classified information such as electronic documents, paper documents, verbally transmitted information, email, information stored on databases and storage media which can be classified in one of the four levels described by Kosutic (2014):

1. Public: This is an information asset that can be accessed by everyone within and outside the organization including people that are not members of the organization.
2. Internal use: This is an information asset that is limited to internal use. Accessibility of this information asset is not allowed for external bodies. This information classification level has the lowest level of confidentiality.
3. Restricted: This information asset is only accessible to selected members of an organization based on their need-to-know and job function.
4. Confidential: Top secrets such as trade secret are classified confidential and should be treated with the highest level of confidentiality within an organization

An asset can be classified into six classes according to ISO 27002 in table 1 below, the first class of asset often referred to as the information asset class; it comprises of printed information, posted or transmitted information, written or spoken information, information shown in films/videos, electronically stored or transmitted information.

The second classification known as the Software assets comprise of operating systems e.g. Windows, Linux Operating system etc., applications built for web or mobile usage, development tools and all other utilities.

Information Asset	Software	Physical Assets and Hardware	Services	People	Intangibles
Printed Information **Written or posted information** **Information Shown in film/Video** **Spoken Conversation** **Electronically stored information** **Electronically transmitted data**	Operating Systems Applications Development tools Utilities	Computer Laptops/iPad/PDAs Mobile phones/Pod USB sticks, CD-ROMs, and backup tapes Copper cables Fiber optics Server Infrastructures	Air-conditioning systems Heating Lighting Internet subscription	Key personnel Qualifications Skills experience	Intellectual Property trademarks Brand Image

Table 1: Asset Classification Based on ISO 27002

The third asset class based on ISO 27002 is the physical assets and hardware which includes assets such as computers, laptops, iPad, PDAs, mobile phones, USB sticks, CD- ROMs and backup tapes as shown in the table.

Fourth asset class includes assets that are considered as services such as heating and cooling services for the data center/ server room, Internet subscription, lighting, and other IT infrastructures related services.

The fifth class of assets are the people involved in the daily operation of the enterprises, it includes all key personnel as well as their various skills, qualifications, and experiences which should be regarded and classified as an asset for the enterprise.

The Intangible class is the last class of the six classes of asset based on the ISO 27002, This class of asset covers all intellectual properties belonging to an enterprise irrespective of its size and type, brand images and trademarks.
Assets are classified according to their value and exposure to enable sensible allocation of budgets and resources where they matter most.

For the board and senior management to effectively manage organization's information assets and the associated risk a well-defined risk management policy should be established. This is because the ultimate responsibility of the board and senior management is to ensure that effective risk management and measures are in place to combat risk. The board can specify the organization's risk tolerance based on its risk appetite to determine when risk should be accepted, reduced, avoided, or transferred in the organization's risk management policy.

Information risk management consists of many processes such that an evaluation of its maturity becomes important. This maturity can be evaluated through the assessment of the organization's current risk management capacity (Jones & Ashenden 2005).

2.4 Determining Gap in Organization's ISG

Developing a roadmap for an organization's ISG requires frequent or annual analysis of the gaps between the current and desired levels to identify organizational perspectives that need improvement as the business environment changes (Brotby 2008). An efficient means of measuring security performance is to identify gaps and devise improvement plan by measuring the organization's maturity using Capability Maturity Model (Szatmary 2015). According to Volchkov (2013) measuring and assessing organizations' security investments is a necessity to justify the return on security investment.

However, the fear of what gap analysis might reveal has made many organizations be unwilling to conduct it. Gap analysis provides an overview of organization's strengths and weaknesses which highlights what an organization does right, and vice versa (Shaw 2012).

The advantages organization stands to gain from determining gaps in ISG process are not limited to its ability to save time and money on irrelevant expenses usually expanded on capabilities that already exist within the organization. Effective gap analysis can help organizations to discover regulatory gaps by identifying specific compliance requirement detailed in the regulatory document.

Failure to regularly conduct a gap analysis to determine and prioritize activities that an organization can correct to achieve its strategic objective might present an overwhelmingly unexpected gap in the organization's ISG process.

Ghaznavi-Zadeh (2018) suggests six important steps that can be used to determine gap and build a roadmap for an organization's information security program these include selecting standard framework e.g. ISO 27000, proper understanding of the business objectives and identifying relevant control perspectives from the standard related to the organization's business processes. Also, customizing the control based on business requirements, determining gap by performing maturity assessment and lastly, developing a program to close the gap in the controls.

2.5 Determining Desired and Current Level of Organization's Information Security

Predetermination of organization's state of information security often enables adequate development of information security strategy. Organizations can achieve this, by envisaging and determining future conditions peculiar to their information security.

The desired state of information security can be achieved by combining different approaches such as capability maturity models, balanced scorecards, information security standards(ISO) 27001:2013 and 27002:2013, and architectural approach because a single approach may not satisfactorily address organization's information security needs.

2.5.1 Capability Maturity Model Approach

A way to characterize the performance and capability of an organization is to measure its capability or maturity. Nath (2016), outlines cost overrun, missed or closed deadlines, poor morale, quality management problems, customers' complaints, and inability to repeat recorded success as some of the consequences of lack of organization's capability.
In the last decades, over 150 capability maturity models have evolved (de Bruin et al. 2005). This is because of the importance of the capability maturity model as a visualization tool for adopting processes and standards, and benchmarking of progress made by organizations (Becker et al. 2009).

The information security management maturity model (ISM^3), NIST information security maturity model developed under the Program Review for Information Security Assistance (PRISMA), and Steven Woodhouse maturity model for Information Security Management systems capability and maturity assessment are among several other models that have been developed to measure organization's capability (Karokola 2011 et al.).

The ISM^3 proposes five (5) maturity level dimensions for information security; Undefined, Defined, Managed, Controlled, and Optimized. Meaning, the capability of an organization's ISG process can be assessed as undefined based on the maturity levels when the governance process is undefined but implementable. For example, an organization may have usable information security governance process which is not defined.

The defined maturity level is attained when the ISG process is documented and used. ISO Standards' process auditing requires organizations to attain "managed level" of maturity to pass capability assessment because organizations should be able to fix and improve defined information security management processes at this level.

The ISG process is better managed and accurate prediction of milestones and resources is achieved when the organization attains a controlled level of maturity. Process improvement and control has been identified as key benefits organizations can derive from optimized maturity level which provides an opportunity for cost savings on resources (ISM3 2007). According to (Karokola et.al. 2011), the limitation of this model is that it does not directly measure security risk and it does not sufficiently address non-technical security issues.

In a similar dimension, NIST (2007) developed a maturity model for the evaluation of information security maturity where five (5) maturity levels of dimensions are named like the ISM^3. In the NIST maturity dimension; policies, procedure, implementation, testing, and integration are the five likely levels of organization's information security maturity. This model is limited by its failure to address non-technical security services.

In another dimension, Steven Woodhouse (2008) argues that the current existing maturity models are not suitable for the assessment of lower levels of maturity below one. Therefore, he proposed a unique maturity model with the following maturity levels dimension; Functional, Technical, Operational, Managed, and Strategic. Steve Woodhouse maturity level dimension consists of additional four layers namely; Negligent (0), Obstructive (-1), Arrogant (-2) and Subversive (-3) that are inconsistent with other maturity level dimensions.

The increasing capability gaps in the previous models are adequately addressed in the Capability Maturity Model Integration (CMMI). This model provides an adaptive framework designed based on best practices for organizations to promote behavior that leads to improved performance. The CMMI consists of five (5) maturity levels for the evaluation of organization's information security maturity; Initial, Managed, Defined, Quantitatively Managed, and Optimizing.

The highest maturity level in the CMMI is the optimizing level characterized by organizations' focus on continuous improvement and ability to respond to change and opportunities. High

maturity indicates organization’s commitment to excellence, high quality, and low-risk information security.
Organizations can expect to move from the initial level of the CMMI by identifying areas of improvements and correcting these areas before integrating the solutions across its business units (Nath 2016).

In Table 2 below, the two COBIT models are different in terms of attributes but can be applied using the same data collection to determine specific gap that needs improvement focus in an organization. However, the COBIT Process Capability Model provides an improved focus and more rigorous process capability assessment than the COBIT Maturity Model.

Information Security Maturity Models	Maturity Levels					
	-3 - 0	1	2	3	4	5
ISM^3	X	Undefined	Defined	Managed	Controlled	Optimized
NIST (PRISMA)	X	Policies	Procedures	Implementation	Testing	Integrating
Steven Woodhouse	Negligent -1: Obstructive -2: Arrogant -3: Subversive	Functional	Technical	Operational	Managed	Strategic
CMMI	X	Initial	Managed	Defined	Quantitatively Managed	Optimizing
COBIT Process Capability Model COBIT 5	Incomplete	Performed	Managed	Established	Predictable	Optimizing
COBIT Maturity Generic Model	Non-existence	Initial /Ad-hoc	Repeatable but intuitive	Defined	Managed and Measurable	Optimized

Table 2: Summary of Maturity Models

COBIT 5 maturity model is based on ISO/IEC 15504 standard and it is based on six maturity levels. This maturity model provides powerful and robust capability evaluation approach as compared to the other maturity models as it does not only give descriptive statement per maturity (De Haes et. al 2013).

2.5.2 Balanced Scorecard Approach

Another approach for implementing organizations' information security is the balanced scorecard. It consists of four management perspectives often used to monitor and evaluate business processes.

According to Kaplan & Norton (1996), the four perspectives of balanced scorecards for profit-oriented organizations are financial, customer, learning and innovation, and internal process. Balanced scorecard financial perspective allows organizations to optimize finance and increase profit by expanding revenues and keeping cost down. The customer perspectives focus on customer satisfaction and retention as means of maintaining organization's reputation.

The way organizations' information security processes are managed based on the expectation of all stakeholders can be recognized from the internal perspective.
The learning and innovation perspectives identify how organizations' staff cultures, capabilities, and skills can be nurtured for receptive learning of current and emerging technologies through training, mentoring, and tutoring.

Non-profit organizations' balanced scorecard is completely different from the profit-oriented organizations. Although, it is equally based on four perspectives; mission, financial recipient, internal processes, and people.
The main driver of non-profit organizations' balanced scorecard is the achievement of organizations' mission. Organizations must consider the beneficiaries of all service offerings to accomplish their mission. Organizations largely depend on people with specific capabilities, skills, and culture to drive some internal processes such as fundraising, financial management, and information security management required for daily operations (Weaver 2016).

2.5.3 Architectural Approach

Traditional Model
Traditionally, the information security strategy implementation is normally forecasted based on the organization's goals or mission or vision. The forecast is often based on past events that occurred in the organization. The main pitfall of the traditional information security model is the heavy reliance on past events without consideration for the current data or changes in industry requirement, making them less adaptive in most organizations.

McKinsey Model

In 1980s, due to the limitations of the traditional models, McKinsey consultants decided to develop an alternative and adaptive model known as the McKinsey Model. This model is based on the theory that the performance of an organization is dependent on how well the seven elements of the model are aligned and mutually reinforced.

The McKinsey model emphasis on the need for the harmonization of strategy, systems, shared values, style, skills, and staff often to achieve organizational objectives (Ravanfar 2015). These elements are divided into soft and hard parts. Strategy, structure, and system form the hard part of the McKinsey model while style, staff, skills, and shared values represent the soft part of the model.

The McKinsey is a Senior Management and Board member’s tool for determining their organization’s strategic alignment. It serves as a monitoring and assessment tool for the determination of internal changes in the organization. The model is commonly used to facilitate change management, acquisition, and merger-related issues in an organization, implement a new strategy, and identify future changes within the organization.

An organization needs to develop strategic plan to gain a sustainable competitive advantage over a short or long-term period. The long-term strategic plan is often recommended for organizations instead of the short term except in situations where the short-term strategic plan can be easily aligned with other 6 elements of the McKinsey model.

Sherwood Applied Business Security Architecture (SABSA) Model

In 1995, a generic layered model and a methodology based on Zachman’s taxonomy for developing risk-driven enterprise information security architectures and for delivering security infrastructure solutions that support critical business initiatives known as SABSA was developed (SABSA homepage).

Successful implementation of the strategic program of information security architecture within any organization can be initiated with SABSA. The SABSA model uses enterprise security architecture approach to address challenges such as poor strategic considerations often experienced in organizations during the design, acquisition, and installation of information security solutions (Sherwood et al. 2009).

According to (Sherwood et al. 2009), the model consists of six layers representing six different views; the business, architect’s, designer’s, builder’s, and tradesman’s and service

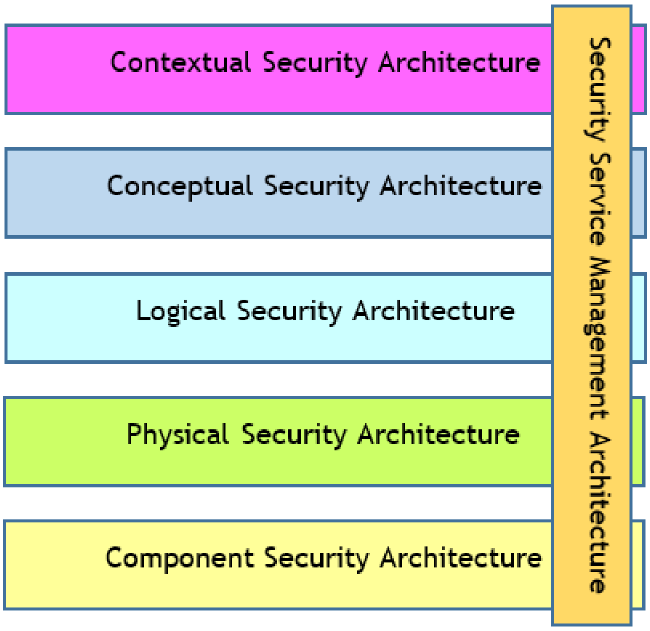

Contextual Security Architecture
Conceptual Security Architecture
Logical Security Architecture
Physical Security Architecture
Component Security Architecture
Security Service Management Architecture

Figure 5: SABSA Architechtural Model Reprinted with the Permission of SABSA Institute

manager's view representing contextual, conceptual, logical, physical, component and security service management architectures as shown in Figure 5 above.

The security service management architecture is vertically placed because security service management issue can be experienced at any of the first five layers.

An organization can create a completely customized information security architecture by using the SABSA matrix with the model. To create this, an organization needs to provide answers to six standard questions asked about information security strategy at each layer of the model.

In the contextual view layer, an organization deals with business requirement analysis and identification of "what" assets the security architecture would be protecting. The answers provided in this layer are taken into consideration in the design and operation of the security architecture. Contextual layer enables business security processes often implemented by the governance and management structure to help manage risk and protect businesses. The overall concept that can be used to meet the business requirement identified in the contextual layer is created at the conceptual view layer. In this layer, Senior management considers "why" the architecture is required for the protection of assets.

In the design view layer, the business is viewed as a system that needs the logical flow of controls where risk management policies and security domains for information assets protection are implemented.

More importantly, an organization needs to consider "how" the security architecture would protect the asset at the logical layer. Additionally, an organization might consider who would be involved in asset protection at the physical layer, where and when to apply security initiatives for assets protection needs to be considered at the component layer, and security service management layer.

2.6 COBIT 5 Framework

Over the years, COBIT has evolved from IT audit to the governance of enterprise IT. In 1991, COBIT was developed by Erik Guldentop and 34 other people who had the invitation to conduct a research to device European IT audit initiative because United States was the only source of IT audit knowledge during this period.

In 1996, COBIT 1 which is the first version of COBIT was issued where COBIT was initially an acronym for Control Objectives for Information and related Technology. However, the term COBIT is not an acronym anymore because COBIT 5 is now a business framework for the governance and management of an organization’s IT (Harmer 2013).

The first version of COBIT known as COBIT1 was an IT audit framework which later became an IT control framework when COBIT2 was issued in 1998. COBIT3 was issued in the year 2000 as an IT management framework. But the governance framework started with the evolution of COBIT4.0/4.1 in the year 2005 followed by COBIT 5 the governance of enterprise IT framework which was introduced in the year 2012.

The COBIT 5 was issued by ISACA, a global business technology association as a comprehensive framework for the alignment of any enterprise business issues through effective governance and management of Information Technology based on globally accepted best practices and models.

The COBIT 5 framework provided five (5) principles for an effective governance and management of Information Technology, which includes; meeting stakeholders need, covering the enterprise end-to-end, applying a single-integrated framework, enabling an integrated approach, and separating governance from management.

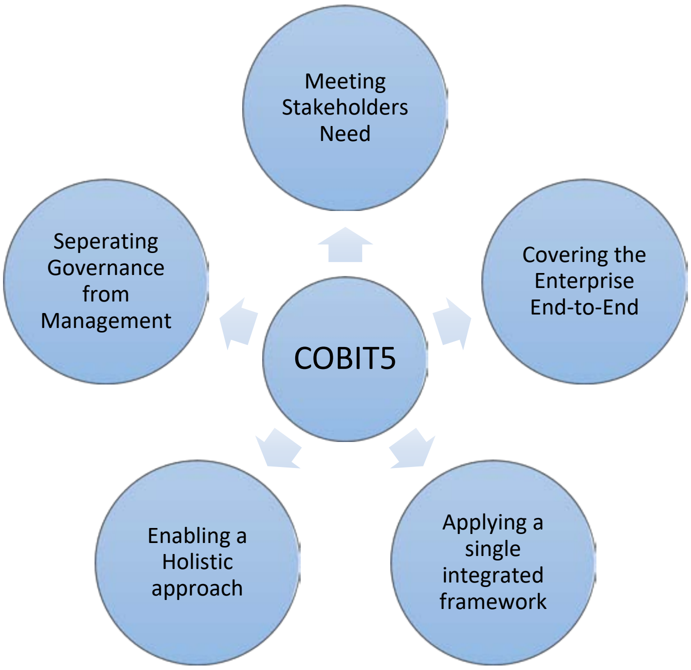

Meeting Stakeholders Need
Covering the Enterprise End-to-End
Applying a single integrated framework
Enabling a Holistic approach
Seperating Governance from Management
COBIT5

Figure 6: COBIT 5 Principles Source: COBIT 5 A Business Framework For The Governance and Management of Enterprise IT-Figure 2

Figure 6 above shows the five principles of COBIT for the governance and management of enterprise IT. According to ISACA 2012, the first principle of COBIT5, emphases the reason for the existence of an Enterprise which is basically to create value for stakeholders. Stakeholders are classified into internal and external stakeholders. The internal stakeholders include; Board members, Business owners, Chief executive officers, Business Managers, Risk Managers, Chief Information Managers, Human resource, IT managers, Security Manager etc while the external stakeholders include; Business Suppliers, shareholders, customers, regulatory body, external auditors, trade union etc.

An enterprise, commercial or non-commercial engages many stakeholders with governance objective of creating value through benefit realization, risk optimization, and resource optimization. Value creation involves realizing benefits -financial for private enterprises, public service for government establishments- at an optimal risk management level while optimizing the resource cost of an enterprise by using goals cascade to translate stakeholders need to actionable strategy.

The second principle provides an end-to-end governance approach for the integration of the enterprise IT governance system into enterprise governance using enablers such as structures, frameworks, processes, practices, and other enterprise’s resources -including people, information, and other IT infrastructures. The governance scope of the end-to-end governance approach must be defined and aligned with the enterprise objective (Value creation), governance enablers, and

3 Research Methodology

This thesis has used both qualitative and quantitative research methodology also known as mixed methods because the combination provides a better understanding of research problems than a single approach (Terell 2012).

3.1 Primary Data Source

Primary data was collected through structured interviews. Josselson (2013) defines interview as a shared product of the interviewer (writer), and the interviewee (the target group) discuss and how they conduct the discussions together. In this case, the target group for interviews were the country representatives and managers representing Organization X in Finland, Sweden, Norway, Denmark, and Iceland. The main justification for the selection of this target group was because they were the process and procedure owners providing management supervision for the perspectives under assessment in the organization.

Respondents	Position	Unit/Country
1	Country Representative	Sweden
2	Country Representative	Finland
3	ICT Manager	All Units
4	Country Representative	Denmark
5	Country Representative	Iceland
6	Secretary	All Units
7	Project Manager	All units
8	Country Representative	Norway

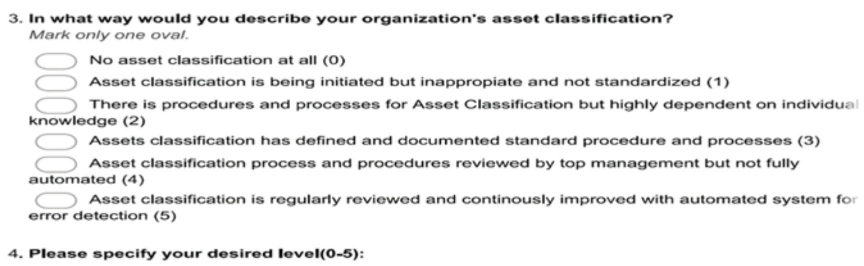
Table 3 List of Country Representatives and Managers Interviewed

The structured interview was found suitable for this research because the interviewer needed answers to series of the same questions from the respondents collected in an orderly and systematic way. The list of respondents interviewed is shown in Table 3.

According to (Cohen & Crabtree 2006), the response category of a structured interview is often limited, and the questions are mostly created before the interview. Generally, structured interviews are characterized by standardized ordering and phrasing of questions which are consistently maintained from one interview to another during the same research exercise. On this basis, a questionnaire was created before the interview to serve as a research instrument.

The interview questionnaire was developed to focus on Seven (7) important perspectives from the ISO/IEC 27002 related to Organization X using COBIT Maturity level dimensions (please see appendix 2 for a sample of the questionnaire). Based on the predefined attributes of each maturity levels from 0 to 5, the following perspectives were discussed in the interview held in Helsinki in March 2018:

- Security policy; respondents were asked to describe their organization's information security policy
- Asset management: respondents were asked to describe their organization's asset classification processes and procedures
- Information Security Incidents: respondents were asked to choose an option that best describes their organization's information security incident management
- Information security risk management: respondents had the option to choose a statement that best described their organization's security culture.
- Supplier Service Delivery Management: Each respondent was given an opportunity to choose a statement that best described their organization's service level agreement management on information systems acquisition development and maintenance.
- Continuity Planning: In this section of the questionnaire respondents were asked to choose an option that best described their organization's continuity planning
- Personnel Security: This is the final section of the questionnaire where respondents were asked to choose a statement that best described their organization's personnel security practices



3. In what way would you describe your organization's asset classification?
Mark only one oval.

○ No asset classification at all (0)
○ Asset classification is being initiated but inappropiate and not standardized (1)
○ There is procedures and processes for Asset Classification but highly dependent on individual knowledge (2)
○ Assets classification has defined and documented standard procedure and processes (3)
○ Asset classification process and procedures reviewed by top management but not fully automated (4)
○ Asset classification is regularly reviewed and continously improved with automated system for error detection (5)

4. Please specify your desired level(0-5):

Figure 7: Sample of a section from the interview questionnaire

The sample of a section from the questionnaire used for the interview is shown in Figure 7. All the seven (7) ISO 27002 perspectives were measured using the COBIT maturity levels as shown in Figure 7. The respondents can only choose one option from the six (6) available options. Each option represents the attribute(s) associated with the COBIT maturity level used to assess the current maturity level. The desired level of each respondent under each perspective was also requested to be provided in the space where respondents were asked to specify their desired level based on COBIT maturity level 0 to 5.

During the interviews, the interviewer provided the questionnaire to each respondent, read out and explained the questions for discussion before the respondents could choose an option considering the attributes in the posters used to explain the levels of maturity. The option and the desired level chosen by each respondent was recorded by the interviewer on the questionnaire.

The data collected under each perspective were recorded on the excel document in Appendix 3. The column 1 of Appendix 3 consists the names of respondents which is numbered 1 to 8 representing the total number of people interviewed. In Appendix 3, the seven (7) ISO perspectives are presented in column 2 to 8, the responses from each respondent were recorded in rows under each perspective from row 2 to 9. Row 10, 11 and 12 contains the current, desired level specified by the organization and the desired levels specified by the respondents respectively. The last row in Appendix 3, shows the maturity level dimensions used.

3.2 Secondary Data Source

The secondary data was collected from relevant information found in the literature. This is because secondary data is usually based on existing data which can be used to provide answers to different research questions (Long-Sutehall et. al 2010). The secondary data source which is also known as literature review is a powerful source for both quantitative and qualitative research because it provides an overview of contributions made by previous researchers. If the literature review is adequately conducted the total research framework is set, and vice versa (Taylor 2000, 46).

3.3 Questionnaire Piloting

The writer conducted a pilot test of the questionnaire on 8th March 2018 at Laurea University of Applied Sciences with 12 participants who are non- members of the Organization X.
The feedback received from the pilot test was used to correct the options in the questionnaire, and determine how to engage participants from Organization X.

During the questionnaire piloting exercise, it was observed that participants exhibited a high tendency for anchoring. Therefore, this unwelcomed tendency was prevented in the actual interview by scheduling different interview time for each respondent from Organization X.

The piloting exercise showed that respondents would be better approached by first, eliciting their organization's desired level of security before the current level. It also shows a need for a thorough explanation of the attributes associated to each maturity level before respondents could start answering the questionnaire. Hence, the need for additional research instrument in form of a poster used to show attributes of each maturity level based on COBIT maturity model (see Appendix 1).

In addition, the poster (Appendix 1) addressed situations in which the options given in the interview questionnaire were not applicable to the respondent or the respondent does not have knowledge by advising the participants to choose the first option. This is because in the COBIT maturity model the first option is indicative of the level of awareness and communication of the perspective within the organization.

The piloting exercise was timed to have an overview of the time required for the actual interview. On this basis, the time required during each interview session was set between 20 to 25 minutes. An important observation during the pilot about the questionnaire was that all participants choose only one option for each question as recommended.

Whilst the questionnaire piloting phase was a success because of the useful feedback received during the session and additional advice on how to conduct the research better yet there was a great lesson learned at the end of the exercise. The filled pilot interview questionnaires received from the participants were unintentionally left in the classroom which could make the integrity of the data collected to be questionable in an ideal interview.

Therefore, the writer developed a checklist of procedures to be observed during the ideal interview sessions which include unboxing the questionnaire at the beginning of the interview and re-boxing it at the end of the interview.

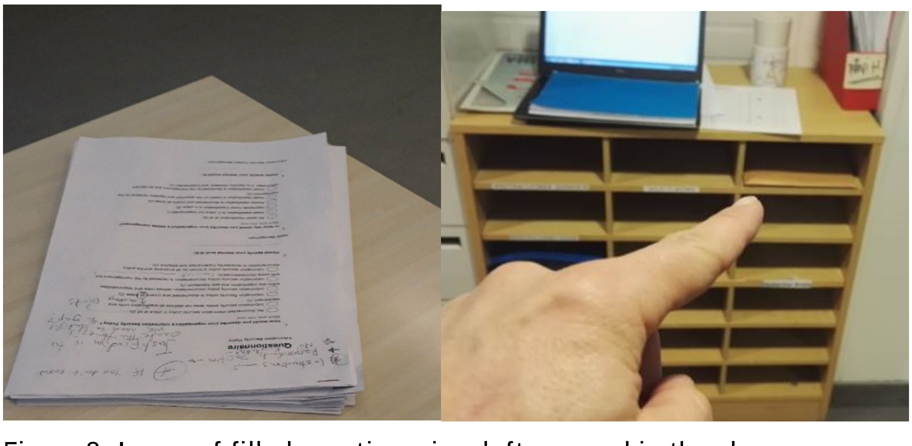


Figure 8: Image of filled questionnaires left exposed in the classroom

3.4 Interview Limitation

The writer strongly relied on Creswell (2013) who suggested that several forms and styles can be used for the qualitative interview. The qualitative interview often involves personal engagement with challenges of meeting, seeing and being seen. In this case, the writer was prepared to meet and see the participants from Organization X.

However, a meeting in the Organization's head office in Stockholm could have provided a field validation of some of the responses gathered.

3.5 Ethical Considerations During the interview

Taylor (2010) outlines four important ethical issues which were considered in this research; First, subject consent to participate in the study must be determined without being forced. The writer gave all participants the choice to determine their participation in the interview and there was no participant under the age of 18 years.

Second, the writer considered the physical and psychological factors which may have a negative impact on the wellbeing of the participants during the questionnaire design, pilot testing phase and the feedback gathered showed no potential harm to participants.

Third, subject privacy was adequately considered, and the questionnaire used for the interviews had no personal information. However, organization's information obtained during the interview will be treated with confidentiality.

Finally, special consideration was taken to ensure participants were not misled during the interviews by providing them information relevant to the research exercise.

4 Findings

This chapter will present the analysis of the data collected during the interviews, and the literature review exercise. This chapter is arranged in two parts, the first part will discuss the qualitative theory-guided analysis, and the second part will elaborate on the quantitive data collected during the structured interviews. Results of the gaps in the organization X's ISG process will be discussed.

From the literature reviewed, it was found that an effective means of determining the gaps in the ISG process of an organization is to assess the maturity level of the processes involved. By assessing the maturity level, the organization's current and desired level of security will be determined as well as the gap between the two levels.

However, there is no universal approach to assess the maturity and identify gaps in the current and desired level of an organization's governance process. The common approaches found in the literature are the capability maturity model, balanced scorecard and the architectural approach.

Although, the capability maturity model has different models developed by different professional institutions such as NIST, ISM3, SABSA, CMMI and ISACA. The literature reviewed shows that COBIT maturity model is a more powerful and robust maturity model than other models. From the data collected during the interview, the gap between the current level and desired levels of Organization X is shown in figure 10 below. During the interview, the data collected through the questionnaire was (2 × 6 × 7) representing a total of 84 data points. More specifically, the 2 represents the current and the desired levels provided by all the respondents during the interview, the 6 represents the possible levels specified by the COBIT maturity model, and the 7 represents the number of perspectives under consideration.

In calculating the current level for each perspective, the simple average of the 8 respondents under each perspective was used. The desired level value of 3 provided by the organization's board was used for each perspective with a strategic implementation period of 2 years.

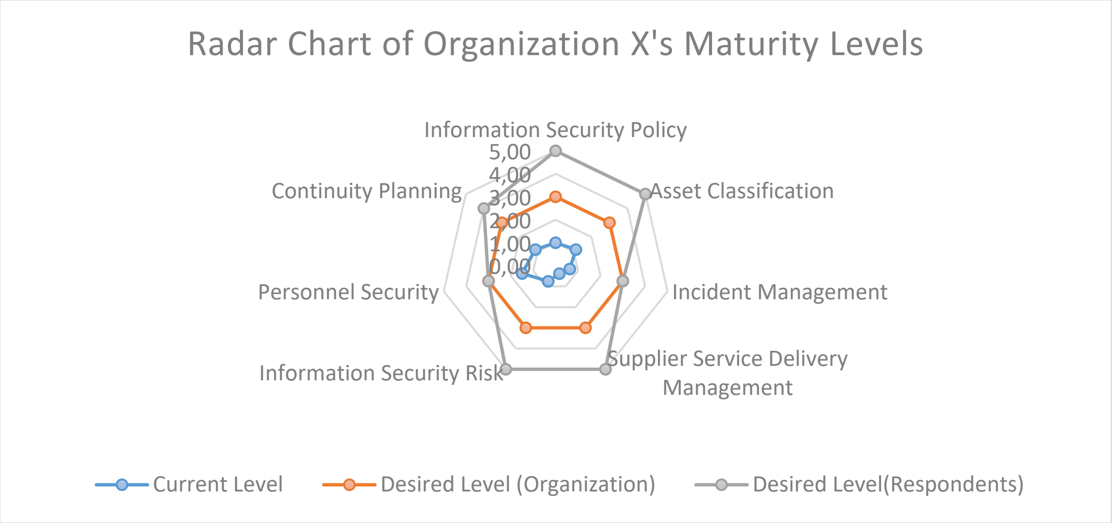


Figure 9: Radar Chart Showing Gaps in Organization X's Maturity Levels

The Radar Chart of Organization X's Maturity levels illustrates the current level, desired levels specified by the organization and the desired level specified by the respondents interviewed. As illustrated in Figure 10, the desired level specified by the organization is a constant value with a COBIT maturity level dimension of 3 for each perspective, which is same as the desired level of personnel security and incident management specified by the respondents. However, there is a wide gap between the desired levels specified by the organization and the respondents in perspectives such as information security policy, asset management service level agreement, information security risk and continuity planning.

The widest gap between the organization's current level and desired level exists in the service level agreement with 2.62 margin, this is followed by the gap that exists in the incident management with 2.37 margin. Similarly, a gap with a margin of 2.25 exists between the current and desired level of the security risk management and an equal gap margin of 1.87 exist between the organization's current and desired asset management, and continuity planning. The narrowest gap exists in the organization's current and desired level of information security policy with a single maturity level margin.

Perspective	Maturity Level Dimension						GAP
	0	1	2	3	4	5	
Information Security Policy		Current ● **1.00**		● Desired			2.00
Asset Classification		● 1.13		●			1.87
Security Risk Management	● 0.75			●			2.62
Incident Management	● 0.63			●			2.37
Supplier Service Delivery Management	● 0.38			●			2.25
Continuity Planning		● 1.13		●			1.87
Personnel Security		● 1.50		●			1.50

Table 4: Summary of Gaps between Organization X's Current and Desired level of ISG

The implication of the gaps between the current and the desired levels will be further discussed. The discussion is arranged in the descending order of the identified gap.

4.1 Supplier Service Delivery Management

As shown in the in Figure 9 and Table 4, the maturity level of Organization X's current supplier service delivery management procedure can be described as non-existence based on the COBIT maturity model.

Theoretically, the current level value of 0.38 indicates that the supplier service delivery is not in existence at all. Meaning Organization X does not have a standardized and defined process and procedures for handling service level agreement. This opinion is shared by 5 out of the 8-people interviewed.

The wide gap and the low current maturity level shown in figure 9 cannot be surprising as earlier findings of a research conducted by IT Policy Compliance Group shows that one out of five organizations do not properly incorporate service requirements, standards, clear definition of ownership of information used by the service providers, and specification of information access rights into the agreements made with the service providers (Meadows 2014).

The incomplete maturity level can be associated with the organization's security risk appetite. From the literature reviewed earlier, risk management was identified as one of the ultimate responsibility of the board and senior executives. Risk identification is an important aspect of the risk management process, it covers identification of risk associated with external parties such as internet service providers, management consultants, cleaning, web developers and hosting service providers, outsourced call services, IT services and cloud service providers.

While an organization with high-risk appetite may not deem it fit to prioritize the establishment of defined processes for managing service level agreements related to third parties and other suppliers, organization with low-risk appetite would consider the criticality and the sensitivity of the information involved, information security policy compliance issues, other service level agreement terms and conditions and most importantly the regulatory and legal issues.

The service level agreement will among many other terms, define the type of access to be given to third parties and other suppliers trading with the organization, termination conditions, the requirement for service continuity, and the rights and conditions for conducting an audit of the agreed terms and defined responsibilities.

The cost-benefit of having a defined process for the service level agreement of organization X cannot be overemphasized when the risk associated with third parties is taken into consideration. Organization X's current level -which is below the initial, managed, and defined level of the COBIT maturity model- indicates that it currently lacks the ability to proactively manage service providers.

Also, it shows the organization's lack of transparency in dealing with service providers because its procedures and processes are not repeatable. It also shows that the organization could sometimes be at loggerheads with third parties because of undefined terms and processes in its service level agreement.

4.2 Incident Management

A closer look at Figure 9 and Table 4 show that Organization X's current level of incident management is at the same level with the current Service Level Agreement even though the existing gap between the current and the desired level of incident management is less than the measured gap under the SLA.

In theory, the current level of the Organization X's incident management can be classified as non-existence based on COBIT maturity level even though five out of 8 people interviewed believe the incident management maturity level is at ad-hoc level.

The interpretation of this maturity level is that Organization X lacks standard processes and procedures as well as defined means of managing incidents. Also, it indicates that Organization X does not only lack sophisticated procedures and standards, it lacks the intuitive capability to effectively manage unforeseen events which might be disruptive to their operations across all the five (5) countries by strategically devising means to minimize the impacts and restore/maintain service delivery.

Unless a proactive step is taken to bridge the gap between the current and the desired level, Organization X may run into huge financial and reputation loss because currently, it lacks standardized and defined processes and procedures to minimize the impacts of both internal and external threats to the confidentiality, integrity, and availability of information assets.

4.3 Information Security Risk Management

Findings from this research have shown that Organization X current information security risk maturity level is at the non-existence level based on COBIT maturity level with a gap value of 2.25 from the organization's desired level. Based on COBIT maturity level, it means that Organization X does not have standardized and defined processes for managing information security-related risk.

The data collected during the interviews clearly indicates that Organization X has some existing processes and procedures for managing information security risk because 5 out of 8 respondents believe that Organization X current level is above the COBIT 5 non-existence level as 4 out of 8 respondents suggested the organization has some processes and procedures for managing information security risk but the processes are not repeatable, and one respondent argues that the processes and procedure is repeatable but highly dependent on individual knowledge which corresponds to level 2 on the COBIT Maturity level. Only 3 out of 8 respondents agree with the current maturity level.

Since the ultimate responsibility and accountability for the effective management of organization's information security risk lies with the Board and the Senior Management as earlier suggested by Jones & Ashenden 2005 in chapter 2 then the current maturity level of Organization X shows that the Board and the Senior Management are not consistently and sufficiently providing strategic direction, developing policy for risk management, deploying appropriate personnel and resources to mitigate risk, and championing organization-wide support for managing regulatory and operational risk. Therefore, it can be concluded that the information security risk of Organization X is poorly governed.

The disadvantages of having a poorly governed information security risk management are clear. The organization will not have the capability to deliver benefit to its stakeholders because a poorly governed information security risk reduces the business value or sometimes adversely destroys the value and causes the organization to miss business opportunities.

The advantages of having a well-governed information security risk management processes and procedures include ease of access to funding and gaining trading partners confidence and reducing the risk of possible damage to organization's reputation and profitability arising from loss of sensitive information assets.

4.4 Information Security Policy

This research has shown that Organization X has information security policy in place, but the policy documentation is not standard because the current level is evaluated to be at the initial/ad-hoc level of the COBIT maturity model based on the responses from 8 people interviewed. At least 7 out of 8 respondents confirmed that the organization has an existing information security policy in place, but it is not supported with sophisticated and standardized procedures and processes.

4.5 Continuity Planning

Findings from this research have shown that Organization X has an existing continuity planning process, but the process is not based on any standard framework. This is because the current level of Organization X's continuity planning maturity level assessment indicates that the organization has already initiated a planning process that will enable it to survive disastrous interruptions and major disasters threatening critical business activities within a restoration time objective.

However, there is a gap of one level between Organization X's current and desired maturity level as shown in Figure 9 and Table 4. This shows that Organization X needs to standardize its continuity planning process without making it highly dependent on individual knowledge. ISO/IEC 27002:2013 recommends that continuity planning procedures and processes are documented. The implementation of this recommendation is especially important for Organization X to bridge the current gap and achieve its desired level.

(Calder & Watkin 2012, 312) emphases the need to test the continuity plan regularly to determine the effectiveness of the documented procedures and processes. The test can be simulated, walk-through, parallel testing in an alternative site or full interruption testing depending on the organization's need based on ISO 27002 recommendation. However, the continuity planning document should be updated with the latest procedures and processes required to effectively and timely restore critical business activities. ISO/IEC 27031:2011 provides comprehensive guidance on continuity planning related to organization's ICT business processes.

4.6 Asset Classification

The main control assessed under this perspective was the Organization X's asset classification. The finding from this research has shown that Organization X has an existing asset classification, but the classification is not based on any standard and it is not supported by any defined procedure and process.
The responses from all the 8-people interviewed during the research show that the current maturity level is at the initial/ad-hoc level on the COBIT maturity model with an approximate gap margin of 2 from the desired level.

4.7 Personnel Security

Finding from this research shows that Organization X does not have defined or standardized Personnel Security process in place but there is an existing arrangement for personnel security. The data collected during the interviews shows that 8 out 8 respondents interviewed believe there is an existing personnel security arrangement in place while 4 out of 8 respondents pointed that the existing personnel security arrangement is highly dependent on the individual knowledge and not standardized. Organization X has a gap of 1.50 margin between its current and desired level of maturity.

5 Conclusions

As mentioned in the introductory chapter, the main purpose of this thesis is to determine the gaps in a non-profit organization's information security governance process and identify the important issues to be considered in developing a roadmap for closing the prevailing identified gaps.

This purpose was achieved in chapter 4, where the presentation of the gap between Organization X's current and desired level of ISG process maturity was presented in table 4 based on the data collected from 8 respondents interviewed.

Perspective	Current Maturity level	Desired Maturity Level	Needed Actions
Supplier Service Delivery Management	0	3	• Create supplier service delivery management procedure • Provide awareness and training on the supplier service delivery management procedures to all affected unit and officials
Incident Management	0	3	• Establish incident Management processes and procedures • provide standard documentation of incidents and management procedures • Provide awareness and training on the processes and procedures to be observed when there is an incident

Information security risk	0	3	• Establish information security risk management process and procedures • Provide standard documentation of information risk-related processes and procedures • Provide awareness and training to all units on the information security risk procedures
Information Security policy	1	3	• Establish standard information security policy based on business objective • Eliminate reliance on individual knowledge and promote organization-wide knowledge sharing • Explicitly define and document the processes and procedures related to information security to the extent of their applicability in each unit
Asset Classification	1	3	• Classify all asset based on likelihood, impact, sensitivity, and criticality • Provide a repeatable process and procedure for asset classification • Document and eliminate high dependence on individual knowledge by providing shared knowledge and training to all concerned parties
Continuity Planning	1	3	• Standardize continuity planning process and procedures based on best practices • Eliminate high reliance on individual knowledge by providing training and knowledge sharing platform for all concerned parties • Define and document processes and procedures

Personnel Security	1	3	• Standardize the existing personnel security management process and procedures • Eliminate dependency on individual knowledge and promote knowledge sharing and training for all concerned parties • Establish a defined process and procedure for personnel security

Table 5: Summary of Needed Actions to be Implemented to close the existing gaps in the Organization X’s ISG

Table 5 above illustrates the current and desired level of maturity of Organization X’s ISG assessed based on COBIT maturity model. Organization X’s current maturity level is summarized in column 2, the desired maturity level is summarized in column 3 and the required actions that needed more focus in the roadmap for closing the existing gaps in Organization X’s ISG are summarized in column 4.

As it can be seen in Table 5, This thesis has shown that Organization X is not completely secure from potential breaches because the non-technical processes and procedures needed to deter, detect, and prevent its information assets from unauthorized access, disclosure, and manipulation are currently not based on any standard practice.

Given the current maturity level of Organization X’s in the three most prioritized perspectives in Table 5; supplier service delivery, incident management and information security risk management which are currently in the non-existence level of the COBIT maturity model, two possible conclusions can be drawn; first, it can be concluded that Organization X has not invested enough resources in these three perspectives; second, it can also be concluded that Organization X has invested some resources on these three perspectives but the investment has not added any positive value to the current profile of the organization and the investment lacks proper communication and awareness sponsorship within Organization X.

Since the procedures and plans involved in the remaining four perspectives namely; information security policy, asset classification, continuity planning and personnel security were not based on any known standards as expressed by the current level of Organization X maturity level under these four perspectives, it can be concluded that Organization X has sufficiently created awareness and communicated its strategic investment on information security policy, asset classification, continuity planning and personnel security to all its business units.

Also, this thesis has shown that for Organization X to attain its desired maturity level, it would need to implement the actions listed in the fourth column of Table 5.
In Chapter 1, the question about the capability of smaller organizations to protect themselves from breaches was raised.

Lastly, this thesis has demonstrated that Organization X's Information Security Governance process is yet to mature to its desired level because there are weaknesses that need to be fixed in its non-technical processes and procedures.

5.1 Thesis Reflection

Conducting an academic research using methodological approach can undauntedly influence a change of status quo. This has been demonstrated with this thesis through a deliberate learning attempt aimed at providing solutions to three key research problems related to a non-profit organization based in the Nordics using the data collected from earlier scholars' publications as a point of departure to finding the gaps in the information security governance process of the non-profit organization as well as identifying important actions needed to close the gaps.

To give more definitive answers to the research problems highlighted in section 1.1 of this report, the writer decided to engage 8 senior managers from the non-profit organization through interview sessions which candidly provided the first-hand information used as the primary data for this thesis. Aside from the data collected for the research purpose during the interviews, it was an opportunity to building strong professional network that cut across 5 countries in the Nordics. Without the interview sessions, the goal of this thesis would have been forfeited as all previous literature reviewed were mostly focused on assessing the gap in the information security governance process of corporate enterprises established for profit making purpose, only few research publications were available on non-profit organization especially the so called NGOs.

Analyzing the data collected and providing a holistic statistical representation of the data can often be daunting, not because of the time and effort that is sometimes required to perform these very important aspects of a thesis especially when quantitative research is used, but because experience gathered from previous learning endeavors is not often transformed into problem solving. This thesis provided an avenue to display knowledge gathered from previous course work in the classroom on numerical and statistical data representation and analysis as evident in section 4, figure 9 and appendix 3 of this report.

The main argument presented at the beginning of this thesis in section 1 was that inadequate information security governance often accommodate inconsistencies in the system configurations and it was associated with the breaches experienced by both profit or non-profit organizations irrespective of the size of the organization. The argument was based on the reports of information security breaches recorded by big companies such as Yahoo, Equifax, eBay etc. Also, the thesis agreed with John Chambers when he concluded that a completely secured data center or network does not exist. The main conclusions of this thesis, drawn in section 5, does not contradict John Chamber's earlier conclusion and the initial argument presented at the beginning of this thesis.

Perhaps, the greatest challenge in this thesis was maintaining anonymity of the non-profit organization that was interested in the thesis for the development of its Information security governance roadmap. However, through proper consultations with research professionals including the thesis supervisor and the representative of the non-profit organization, a solution was reached on how to uphold anonymity without undermining the validity and reliability of the thesis findings.

While there were several lessons learned during this thesis, two seems highly significant to the successful completion of the research process. Firstly, the guidance sessions between the thesis writer and the supervisor. The discussions and suggestions from the sessions influenced the thesis writer's style of specifying the needed actions to close the identified gaps in the non-profit organization's information security governance process shown in Table 5. Secondly, conducting a pilot of the data collection approach can have a positive influence on the conduct of the actual data collection. This thesis was a proof on how piloting can help to raise any researchers' consciousness to salient ethical aspect of research. A narration about the writer's experience during the questionnaire piloting phase was presented in section 3.3.

Finally, it is important to note that the experience from the questionnaire piloting phase reported in section 3.3 of this report does not undermine the findings of this thesis because the pilot was only a preparatory exercise towards the actual interviews.

5.2 Recommendation

This thesis would recommend that the current maturity levels already achieved in areas such as information security policy, asset classification, continuity planning and most importantly personnel security can be improved by standardizing and defining the process and procedures involved in each perspective. Organization X should consider the cost and benefit of moving from each current level already attained to the next and the desired level. If the cost needed to move to the desired level is more than the benefits, then the current maturity level should be sustained until the benefits out-ways the cost.

Also, this thesis would strongly recommend that Organization X should address the gap identified in its information security policy first as every other perspective assessed in this thesis are dependent on how the information security policy is perfectly aligned with the strategic business objective of the organization.

Finally, this thesis would recommend a more rigorous process capability assessment of Organization X ISG supported by field study of all the units in the Nordics to determine if the organization needs the present desired maturity level in all the perspectives assessed in this thesis.

References

Printed Sources

Creswell, J.C. 2013. Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. London: Sage Publications

Donaldson, S. E., Siegel, S. G., Williams, C. K. & Aslam, A. 2015. Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats. New York: Apress

Harmer, G. 2013. Governance of Enterprise IT Based on COBIT 5: A Management Guide. Ely, Cambridgeshire, U.K: IT Governance Pub.

Jones, A. & Ashenden, D. 2005. Risk Management for Computer Security: Protecting Your Network and Information Assets. Oxford: Elsevier

Josselson, R. 2013. Interviewing for Qualitative Inquiry: A Relational Approach. New York: The Guilford Press

Kaplan, R. S., & Norton, D. P., 1996. The Balanced Scorecard: Translating Strategy into Action. Cambridge: Harvard Business Press

Peltier, T. R. 2002. Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management. Florida: CRC Press

Taylor, G. R. 2010. Integrating Quantitative and Qualitative Methods in Research. New York: University Press of America

Touhill, G. J., & Touhill C. J. 2014. Cybersecurity for Executives: A Practical Guide. New Jersey: Wiley

Whitman, M. E., & Mattord, H. J. 2016. Management of Information Security: Fifth Edition. Boston: Cengage Learning

Electronic Sources

Becker, J., Knackstedt, R., & Pöppelbuß, J. 2009. Developing maturity models for IT management. Business Information Systems Engineering-Research Paper. Volume 1(3):213–22. Accessed February 22 2018 https://link.springer.com/content/pdf/10.1007%2Fs12599-009-0044-5.pdf

Brotby, W. K. 2008. Information Security Governance: Guidance for Information Security Managers. Article from IT Governance Institute, Accessed 11 November 2017. http://isaca.org

Cassidy, A. 2006. A Practical Guide to Information Systems Strategic Planning: 2nd ed. Accessed 3 December 2017. http://dinus.ac.id/repository/docs/ajar/Anita_Cassidy__A_Practical_Guide_to_Information_Systems_Strategic_Planning__Second_Edition.pdf

Chew, Eng., K. & Gottschalk, P. 2009. Information Technology Strategy and Management: Best Practices. Accessed 23 November 2017. http://isaca.org

Cohen, D. & Crabtree, B. 2006. Qualitative Research Guidelines Project. Accessed 05 March 2018 http://www.qualres.org/HomeStru-3628.html

Conner, B. & Swindle, O. 2004. The Link Between Information Security and Corporate Governance. Computerworld. Accessed 20 February 2018. https://www.computerworld.com/article/2564800/security0/the-link-between-information-security-and-corporate-governance.html

de Bruin, T., Freeze, Ron., Kulkarni, U., & Rosemann, M. 2005. "Understanding the Main Phases of Developing a Maturity Assessment Model" ACIS 2005 Proceedings. 109. accessed 03 March 2018. https://aisel.aisnet.org/acis2005/109

De Haes, S., and Van Grembergen, W. 2009. An Exploratory Study into IT Governance Implementations and Its Impact on Business/IT Alignment, 26(2), 123-137 Article from EBSCO Business Source Elite. Accessed 29 March 2018. http://search.ebscohost.com.nelli.laurea.fi/login.aspx?direct=true&db=bsh&AN=37604194&site=ehost-live

De Haes, S., Debreceny, R., & Van Grembergen, W. 2013. Cobit Process Maturity and Process Capability. ISACA Journals Author blog. Accessed 01 March 2018. https://www.isaca.org/Journal/Blog/Lists/Posts/Post.aspx?ID=197

Delligent Corporations., 2016. Five Best Practices for Information Security Governance. Accessed 10 March 2018. http://diligent.com/wp-content/uploads/2016/10/WP0018_UK_Five-Best-Practices-for-Information-Security-Governance.pdf

Hann, J. & Weber, R. 1996. Information Systems Planning: A Model and Empirical Tests. Management Science. Accessed 24 April 2018. https://pubsonline.informs.org/doi/pdf/10.1287/mnsc.42.7.1043

Gelbstein, E. 2012. Strengthening Information Security Governance. ISACA Journal (2). Accessed 12 March 2018. https://www.isaca.org/Journal/archives/2012/Volume-2/Documents/12v2-Strengthening-Information.pdf

Gelles, D. 2015. Executives in Davos Express Worries Over More Disruptive Cyberattacks. Dealbook. Accessed 22 November 2017. https://dealbook.nytimes.com/2015/01/22/in-davos-executives-express-worries-over-more-disruptive-cyberattacks/

Ghaznavi-Zadeh, R. 2018. Information Security Architecture: Gap Assessment and Prioritization, ISACA Journal (2). Accessed 27 March 2018. https://www.isaca.org/Journal/archives/2018/Volume-2/Pages/information-security-architecture.aspx

Henderson, J. C. & Venkertraman, H. 1993: Strategic Alignment Leveraging Information Technology for Transforming Organizations. IBM Systems Journal, 32(1), 4 Accessed 4 November 2017. https://pdfs.semanticscholar.org/e840/2b65103442e2517982e5e3eb330f72886731.pdf

ISACA 2012. COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. Accessed 14 March 2018. http://www.isaca.org/cobit/Pages/CobitFramework.aspx

ISM^3 Consortium 2007. ISM3 Information Security Management Maturity Model Handbook. Accessed 21 February 2017. https://www.lean.org/FuseTalk/Forum/Attachments/ISM3_v2.00-HandBook.pdf

Karokola, G., Kowalski, S., & Yngström, L. 2011. Towards an Information Security Maturity Model for Secure e-Government Services: A Stakeholders View. Accessed23 February 2018. http://www.diva-ptal.org/smash/get/diva2:469623/FULLTEXT02.pdf

Kearney, W. D., & Kruger, H. A. (2013). A framework for Good Corporate Governance and Organizational Learning: An empirical study. International Journal of Cybersecurity and Digital Forensics (2), 36-47. Accessed 19 December 2018 http://sdiwc.net

Kosutic, D. 2014. Information Classification According to ISO 27001. Advisera. Accessed 24 March 2018. https://advisera.com/27001academy/blog/2014/05/12/information-classification-according-to-iso-27001/

Long-Sutehall, T., Sque, M & Addington-Hall, J., 2010. Secondary Analysis of Qualitative data: A valuable Method for Exploring Sensitive Issues with an elusive population. Journal of Research in Nursing. Accessed 02 March 2018. https://www.wlv.ac.uk/media/wlv/pdf/Secondary-analysis-JRN3815531.pdf

Meadows, R. 2014. ISACA Helps Enterprises Manage Vendors Using the COBIT 5 Framework: Guide Provides Samples SLAs, Case Studies Mappings. ISACA Press Release. Accessed 19 March 2018. https://www.isaca.org/About-ISACA/Press-room/News-Releases/2014/Pages/ISACA-Helps-Enterprises-Manage-Vendors-Using-the-COBIT-5-Framework.aspx

Nath, S. 2016. Building Capacity with CMMI. ISACA Now Blog. Accessed 01 March 2018. https://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=667

NIST 2006. Information Security Handbook: A Guide for Managers. NIST Special publication 800-100. Accessed 21 February, 2018. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf

Obicci, M. & Adoko, P. 2017. Risk Management Strategy in Public and Private Partnerships. Accessed 23 November 2017.

https://books.google.fi/books?id=1T5IDgAAQBAJ&lpg=PA128&dq=risk%20is%20an%20intrinsic%20part%20of%20all%20organization&hl=fi&pg=PA128#v=onepage&q&f=false

Osborne, M. 2006. How to Cheat at Managing Information Security. Rockland: William Andrew, Accessed 24 April 2018. https://ebookcentral.proquest.com

Pironti, J.P. 2010. Developing an Information Security and Risk Management Strategy. ISACA journal (2), Accessed 23 November 2017. https://www.isaca.org/Journal/archives/2010/Volume-2/Documents/jpdf1002-developing-an-infor.pdf

Ponemon Institute. 2017. 2017 Cost of Data Breach Study: Global Overview. Accessed 24 April 2018. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN

PwC GSISS, 2018. Global State of Information Security Survey. Accessed 21 February 2018. https://www.pwc.com/us/en/cybersecurity/assets/pwc-strengthening-digital-society-against-cyber-shocks.pdf

Ravanfar M. M. 2015. Analyzing Organizational Structure Based on 7s Model of McKinsey. Global Journal of Management and Business Research: An Administration and Management, Volume 15, Issue 10 version 1.0. Global Journal Inc: USA Accessed 21 February 2018. https://pdfs.semanticscholar.org/9fd1/4d415ed96b1dcafa9d84ddde97ecabe5dbda.pdf

Sabherwal, R. & Chan, Y. E. 2001. Alignment between business and IS strategies: A study of prospectors, analyzers, and defenders. Information Systems Research, 12(1), 11-33.

Shaw, R., 2012. Conducting an Information Security Gap Analysis. Accessed 11 March 2018. https://images.template.net/wp-content/uploads/2016/01/04125735/Information-Security-Gap-Analysis-PDF-Format-Download.pdf

Sherwood, J., Clark, A., & Lynas, D. 2009. Enterprise Security Architecture. SABSA Institute White Paper. Accessed 2 March 2018. http://www.mitsconsulting.com/images/SABSA_White_Paper_2009.pdf

Szatmary, E. 2015. Defining and Measuring Capability Maturity for Security Monitoring Practices: Dell SecureWorks Incident Response and Digital Forensics. Accessed 11 March 2018. https://www.first.org/resources/papers/conf2015/first_2015_szatmary-eric_defining-and-measuring-capability-maturity_20150625.pdf

Terell, S. R. 2012. Mixed-Method Research Methodologies: *The Qualitative Report*, *17*(1), 254-280. Accessed 30 October 2017. http://nsuworks.nova.edu/tqr/vol17/iss1/14?utm_source=nsuworks.nova.edu%2Ftqr%2Fvol17%2Fiss1%2F14&utm_medium=PDF&utm_campaign=PDFCoverPages

Volchkov, A. 2013. How to Measure Security from Governance Perspective. ISACA Journal (5), Accessed 11 March 2018. https://www.isaca.org/Journal/archives/2013/Volume-5/Documents/How-to-Measure-Security-From-a-Governance-Perspective_jrn_English_0913.pdf

Von Solms, R. & Von Solms, (Basie) S. H. 2006. Information Security Governance: A model Based on the Direct-Control Cycle. Computers and Security Journal (25)6, 408-412. Accessed 24 April 2018. http://www.sciencedirect.com/science/article/pii/S0167404806001167

Watkins, S., & Calder, A. (2010). Information security risk management for ISO 27001/ ISO27002. Accessed 19 February 2017. https://ebookcentral.proquest.com

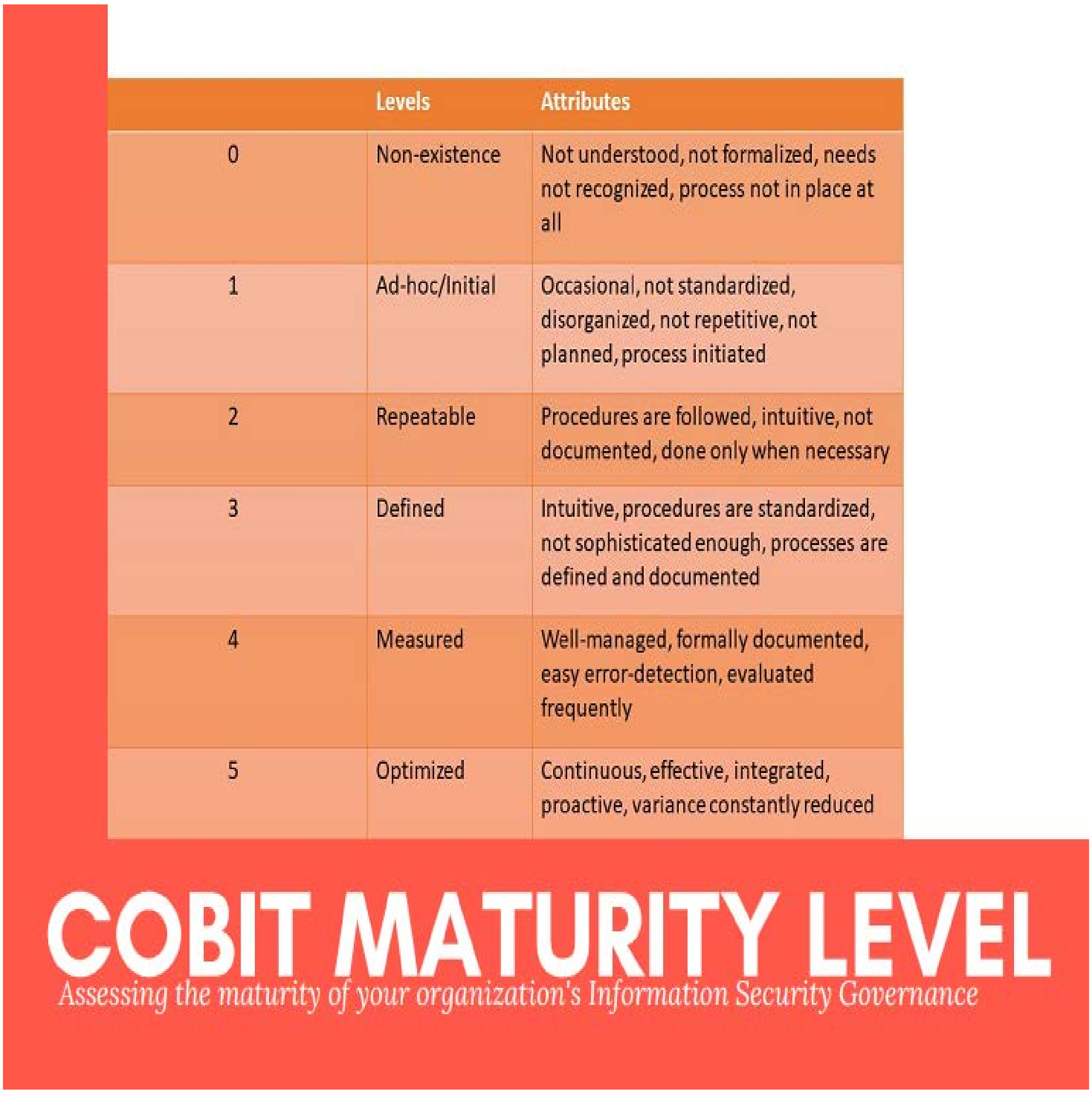
Weaver, J. 2016. The 4 Balanced Scorecard Perspectives: An Overview for Manager. ClearPoint Strategy. Accessed 01 March 2018. https://www.clearpointstrategy.com/balanced-scorecard-perspectives/

Figures

Tables

Appendices

Appendix 1: Poster of COBIT Maturity Level Used During the Interview

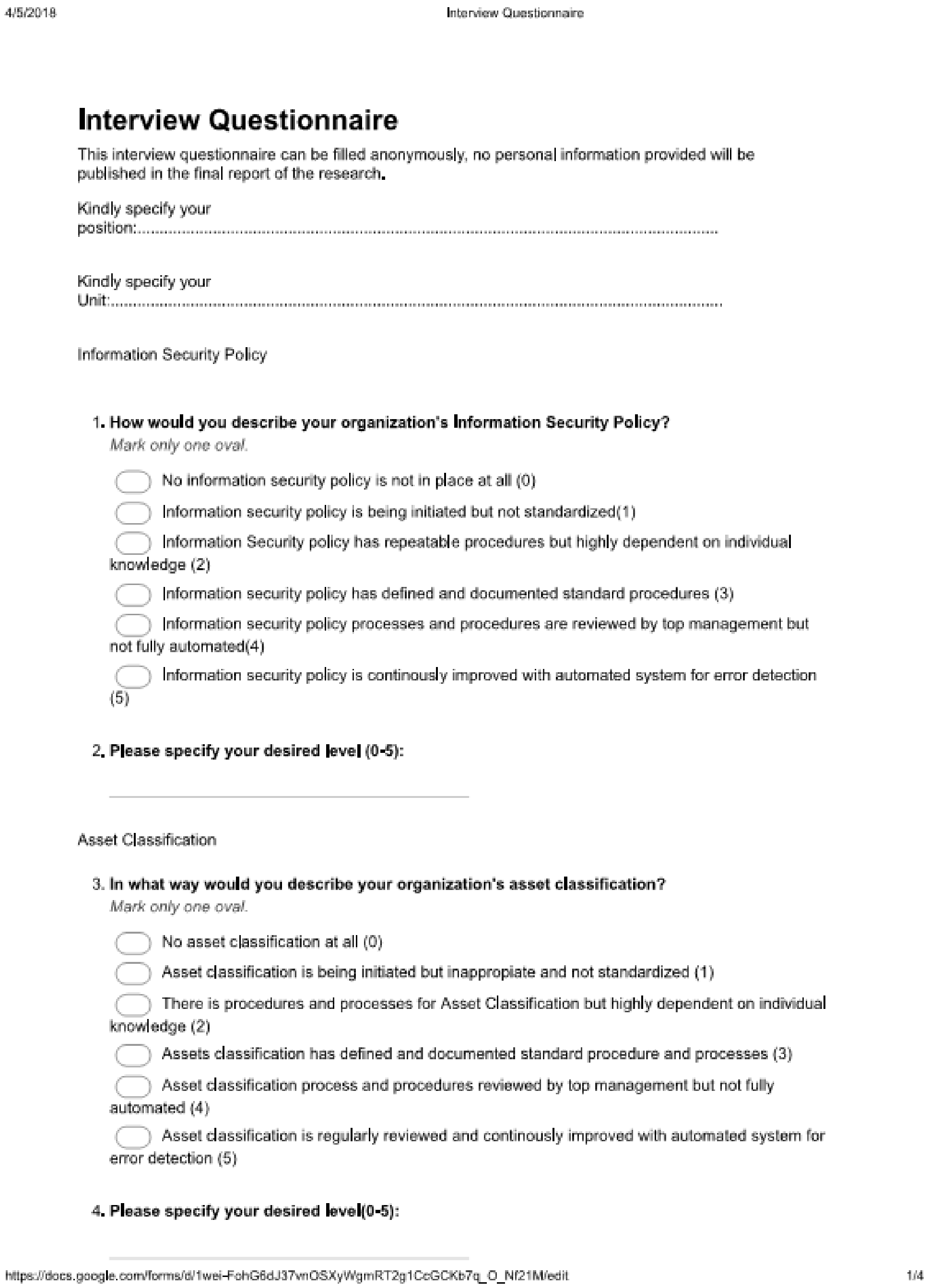


	Levels	Attributes
0	Non-existence	Not understood, not formalized, needs not recognized, process not in place at all
1	Ad-hoc/Initial	Occasional, not standardized, disorganized, not repetitive, not planned, process initiated
2	Repeatable	Procedures are followed, intuitive, not documented, done only when necessary
3	Defined	Intuitive, procedures are standardized, not sophisticated enough, processes are defined and documented
4	Measured	Well-managed, formally documented, easy error-detection, evaluated frequently
5	Optimized	Continuous, effective, integrated, proactive, variance constantly reduced

COBIT MATURITY LEVEL

Assessing the maturity of your organization's Information Security Governance

Appendix 2: The Questionnaire Used for the Interview



4/5/2018 Interview Questionnaire

Interview Questionnaire

This interview questionnaire can be filled anonymously, no personal information provided will be published in the final report of the research.

Kindly specify your position:...

Kindly specify your Unit:...

Information Security Policy

1. **How would you describe your organization's Information Security Policy?**
Mark only one oval.

○ No information security policy is not in place at all (0)

○ Information security policy is being initiated but not standardized(1)

○ Information Security policy has repeatable procedures but highly dependent on individual knowledge (2)

○ Information security policy has defined and documented standard procedures (3)

○ Information security policy processes and procedures are reviewed by top management but not fully automated(4)

○ Information security policy is continously improved with automated system for error detection (5)

2. **Please specify your desired level (0-5):**

____

Asset Classification

3. **In what way would you describe your organization's asset classification?**
Mark only one oval.

○ No asset classification at all (0)

○ Asset classification is being initiated but inappropiate and not standardized (1)

○ There is procedures and processes for Asset Classification but highly dependent on individual knowledge (2)

○ Assets classification has defined and documented standard procedure and processes (3)

○ Asset classification process and procedures reviewed by top management but not fully automated (4)

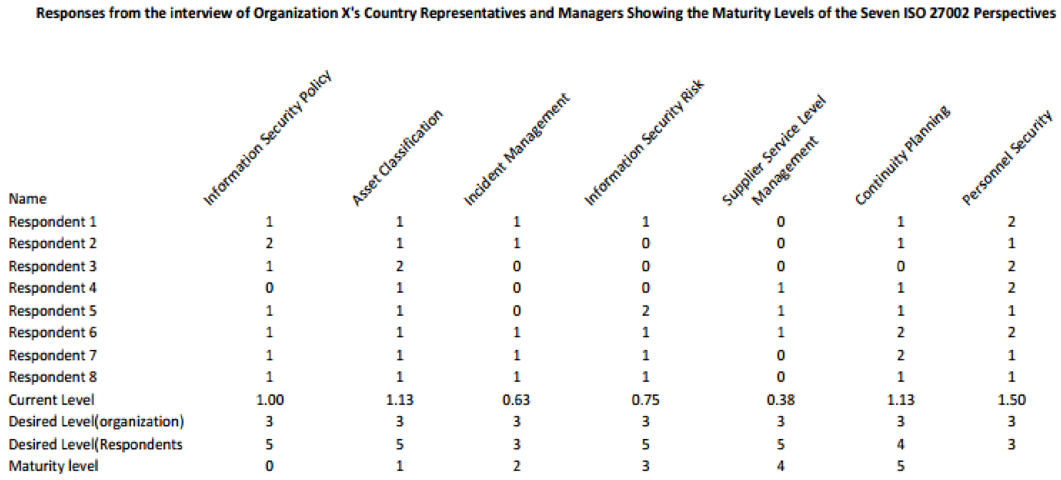
○ Asset classification is regularly reviewed and continously improved with automated system for error detection (5)

4. **Please specify your desired level(0-5):**

____

https://docs.google.com/forms/d/1wei-FohG6dJ37vnOSXyWgmRT2g1CcGCKb7q_O_Nf21M/edit 1/4

Appendix 3: Responses from the Interviews conducted with the Country Representatives and Managers of Organization X



Responses from the interview of Organization X's Country Representatives and Managers Showing the Maturity Levels of the Seven ISO 27002 Perspectives

Name	Information Security Policy	Asset Classification	Incident Management	Information Security Risk	Supplier Service Level Management	Continuity Planning	Personnel Security
Respondent 1	1	1	1	1	0	1	2
Respondent 2	2	1	1	0	0	1	1
Respondent 3	1	2	0	0	0	0	2
Respondent 4	0	1	0	0	1	1	2
Respondent 5	1	1	0	2	1	1	1
Respondent 6	1	1	1	1	1	2	2
Respondent 7	1	1	1	1	0	2	1
Respondent 8	1	1	1	1	0	1	1
Current Level	1.00	1.13	0.63	0.75	0.38	1.13	1.50
Desired Level(organization)	3	3	3	3	3	3	3
Desired Level(Respondents	5	5	3	5	5	4	3
Maturity level	0	1	2	3	4	5	